DOE CIO Guidance CS-23

U.S. Department of Energy

Cyber Security Program

PEER TO PEER (P2P) NETWORKING GUIDANCE

December 2006

This Guidance document was developed and issued outside of the Departmental Directives Program.

1. PURPOSE.

   There are numerous descriptions of P2P: a communications model in which each party has the same capabilities and either party can initiate a communication session; a method of direct communication or collaboration (mostly file-sharing) between computers, where none are simply client or server, but all machines are equals; or a type of file sharing software or system allowing individual users of the Internet to connect to each other and trade files. Frequently, the P2P application is a combined server and client that does not require identification and authentication by a user or make connections to other systems within the network. These types of applications present a significant security issues to the computer resources of the Federal Government.

   Peer-to-peer (P2P) technology/services/applications are useful but introduce significant security risks that must be mitigated to maintain the security of DOE systems and networks. This Department of Energy (DOE) Chief Information Officer (CIO) Guidance applies Office of Management and Budget Memorandum 04-26, *Personal Use Policies and "File Sharing" Technology*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems,* and other applicable Departmental and Federal information technology security laws and regulations.

   The DOE Office of the Chief Information Officer (OCIO) will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

   This Guidance is provided to Senior DOE Management for addressing the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance,* and DOE Manual 205.1-4, *National Security Systems Controls Manual*, in their Program Cyber Security Plans. Specifically, this Guidance applies to Access Control; Awareness and Training; Certification, Accreditation, and Security Assessment; Configuration Management; Identification and Authentication; Risk Assessment; System and Communication Protection; and System and Information Integrity; User Data Protection; Configuration Management; Operational; Delivery and Operational; Development; Life Cycle; and Vulnerability Assessment controls in those documents.

3. CANCELLATIONS.

   None

4. APPLICABILITY.

   a. Primary DOE Organizations. This guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to Which DOE CIO Guidance CS-23 is Applicable*.

      Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within its operating units and is responsible for ensuring that those requirements are incorporated into contracts.

   b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.

   c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems hosting unclassified information. DOE CIO Guidance CS-38A, *Protection of Sensitive Unclassified Information, including Personally Identifiable Information Guidance*, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.

   d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM);* the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information.. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

   This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its issuance. If Senior DOE Management cannot address all of the criteria by that date, Senior DOE

Management is to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance into their PCSPs.

6. CRITERIA.

   a. P2P applications are not to be used on DOE systems that contain or process Sensitive Unclassified Information (SUI). The default condition is that no P2P technology or services are to be used except under conditions prescribed by Senior DOE Management in their PCSPs.

   b. Program Cyber Security Plan. Senior DOE Management PCSPs must define the conditions under which P2P technology and services may be implemented and require operating units that deploy P2P to develop, document, and implement policies and procedures the following criteria and commensurate with the level of security required for the organization's operating environment(s) and specific mission needs.

      (1) If the application of P2P technology or service is required in networks each application must be justified and approved by Senior DOE Management. The justification must, as a minimum, include the following:

         (a) Risk assessments for systems where P2P technology or services are to be used.

         (b) Description of the P2P protocol(s) and application.

         (c) Identification of controls at the system and network levels to detect improper use and attempted evasion of security measures.

      (2) The following security controls are to be implemented on applications, system components, and networks that are part of, or may come into contact with, P2P applications, technology, or services. Implemented controls are to be tested and documented in all associated System Security Plan(s).

         (a) Technical controls that do not allow the P2P server-client applications to reply (e.g. Pong) to broadcasts for locating another server-client (e.g. Pings).

         (b) Operational controls detailing procedures for handling and distributing information.

         (c) Management controls describing the rules of behavior for the user in using the technology or service.

         (d) Protocols specific to P2P server-client applications are not passed on the network unless specifically authorized for each system hosting a P2P server-client application.

(e) Technical controls that provide the capability to detect and block unauthorized P2P applications, services, and software ports.

(f) P2P access controls that reflect the Information Types and Security Category of the system.

(g) Technical controls that limit operation of the server-client application to downloading and does not allow writing to the disks on the system hosting the P2P application From another system or system component.

(h) Technical controls that limit the ports used by P2P applications.

c. Criteria Unique to National Security Systems.

P2P applications present an unacceptable level of risk to any system or network that contains or processes classified information. Therefore, P2P applications are prohibited from being employed in any DOE National Security System.

7. REFERENCES.

References are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

8. DEFINITIONS.

Peer-to-Peer (P2P) Network. A peer-to-peer computer network is a network that relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers. Each computer has the same capabilities and either party can initiate a communication session.

Server-client Application. An application that incorporates the functionality of a client and server.

Other acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

9. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1:

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS-23 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Health, Safety, and Security
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration